

USAWC STRATEGY RESEARCH PROJECT

ALWAYS ON: ACHILLES HEEL OF THE NETWORKED FORCE?

by

Lieutenant Colonel Michael T. Barry
United States Marine Corps Reserve

Colonel David J. Smith, USA
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page			Form Approved OMB No. 0704-0188		
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 30 MAR 2007		2. REPORT TYPE Strategy Research Project		3. DATES COVERED 00-00-2006 to 00-00-2007	
4. TITLE AND SUBTITLE Always On Achilles Heel of the Networked Force?				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Michael Barry				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army War College, Carlisle Barracks, Carlisle, PA, 17013-5050				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT See attached.					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 21	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

ABSTRACT

AUTHOR: Lieutenant Colonel Michael T. Barry

TITLE: Always On: Achilles Heel of the Networked Force?

FORMAT: Strategy Research Project

DATE: 30 March 2007 WORD COUNT: 5817 PAGES: 21

KEY TERMS: Communications, Transmission Security, Radio Direction Finding, Spectral Analysis, Network-centric Warfare, Globalization

CLASSIFICATION: Unclassified

Thoroughly enamored with the benefits of exchanging information in near-real-time, the U.S. military has committed itself to networking the battlefield. Brought about by the convergence of military and consumer communications technology, the networked battlefield boasts continuous connectivity with digitized information. However, the network-centric force is reliant on the radio frequency spectrum to pass information, and is “always-on,” which is to say, it is constantly producing radio frequency emissions in order to share information in near-real-time. Historical experience should not be ignored. Passive radio transmission detection techniques have been used since the dawn of radio to achieve decisive results. The Achilles heel of the networked force is that it is always-on, continuously exposed to detection. Recommendations are advanced to quantify this awkward vulnerability, train and educate for more decentralized command and control, and focus effort on developing a primarily passive, rather than transmission dependent, situational awareness architecture.

ALWAYS ON: ACHILLES HEEL OF THE NETWORKED FORCE?

"We were able to monitor Israeli communications, and we used this information to adjust our planning."

—a Hezbollah commander, Lebanon, 2006¹

The current military communications environment is characterized by radio systems which continuously transmit and receive information, resulting in near-real-time information exchange which has significantly increased battlefield situational awareness. This has been achieved, in part, through the fielding of several automated force tracking systems, such as the Force XXI Battle Command Brigade and Below/Blue Force Tracker transceiver (FBCB2-BFT) and the Movement Tracking System (MTS). The trend toward networking all warfighters with the information that enables them to rapidly assess a situation and make timely decisions continues unabated.²

The rapid adaptation of these systems over the past decade, along with a variety of tactical radios, wireless data-linked Intelligence, Surveillance, and Reconnaissance (ISR) platforms, radio-controlled robots, and a growing catalog of radio-enabled battlefield sensors, reflect a fundamental change in the use of radio frequency spectrum on the modern battlefield. The fundamental change is this: the network-centric force is "always-on," which is to say, it is constantly producing radio frequency emissions in order to effectively share information in near-real-time.

Unfortunately, this networked, always-on communications environment has encouraged a relaxed, desensitized approach toward radio transmission security. Joint Publication 1-02 defines transmission security as, "The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis."³ Radio communications are essential to sharing information within the battlefield communications environment and transmission security entails those actions taken to prevent friendly signals from being detected. A desensitized approach to transmission security presents potential adversaries with an opportunity to leverage commercially available technologies to passively conduct Radio Direction Finding (RDF) and radio frequency traffic analysis in order to more accurately choose the time and place to seek decisive action.

The risks assumed in forgoing transmission security might appear to be offset by the advantages gained with a networked, always-on force--especially in traditional forms of land warfare. These undisputed advantages include increased combat power, synchronized

battlefield effects, speed of command, increased lethality, survivability, and responsiveness.⁴ They contribute to the fact that the United States has no global peer competitor in traditional military capability.⁵ The technical enabler of these advantages is the ability to transmit and receive information in near-real-time, providing commanders with enhanced battlefield situational awareness. The resulting shared situational awareness, or Common Operational Picture (COP), is derived from transmissions which are essentially continuous, or always-on.

It's unlikely that potential adversaries will allow this capability to go unchallenged. The National Military Strategy states that the "Global proliferation of a wide range of technology will affect the character of future conflict."⁶ A forecast of future conflict ought necessarily to include enemy actions taken to mitigate the advantages of pervasive battlefield situational awareness made possible by persistent communications. Colin Gray states, "No polity, including the United States today, ever is permitted to enjoy for long, unchallenged, the benefits of a successful revolutionary way in warfare."⁷ The challenge for US forces is to ensure military effectiveness in the face of emergent styles of warfare that employ the same fundamental, globally sourced, dual-use technologies that have produced the advantages of the networked, always-on force.

In the radio frequency domain, the historical record provides ample reference to the use of passive RDF techniques in achieving decisive results. The assumption that an adversary can not, or will not use passive radio direction-finding and spectral analysis techniques to detect the proximity and disposition of the current and future networked force, and use this knowledge to adjust his plans, may already be proving dangerously short-sighted. The Achilles heel of the networked force is that it is always-on, continuously exposed to detection. This awkward vulnerability needs to be quantified, training and education must lead to more decentralized command and control, and priority assigned to developing primarily passive, rather than transmission dependent, situational awareness communications architectures.

The Historical Experience

The same principles of transmission detection used by the U.S., its allies, and adversaries to gain military advantage in conflicts throughout the 20th century can be applied today. A review of radio communications from its inception just over a century ago reveals that the command and control advantages obtained through the use of radio were consistently challenged, and often countered, with adaptive signal detection techniques developed from the same fundamental technology.

The first documented work on the use of antennas for direction finding was conducted in 1904, just sixteen years after Heinrich Rudolf Hertz succeeded in transmitting the first radio

wave.⁸ Bellini and Tosi improved the work by fabricating the first radio direction finding apparatus. As improved communications became a feature of military command and control during World War I, the refinement of RDF equipment continued. For example, the Royal Navy employed RDF to detect a critical movement of the German High Seas Fleet and subsequently committed the British fleet to battle at Jutland, achieving a decisive result. For the remainder of the war, the Royal Navy was not threatened on the high seas by the German fleet.⁹ The British experience with RDF proved the value of technical discovery in an entirely new realm of science, which held promise for tremendous impact in the conduct of war.

The period between the two world wars was marked by broad technical innovation resulting in radar, wireless communications technology, and High Frequency Direction Finding (huff-duff).¹⁰ These advances, together with the evolution of integrated RDF techniques with operational plans, significantly influenced the conduct of operations during the Second World War. The experience of World War II suggests that whenever new capabilities were introduced in the realm of radio communications, they were soon met with counter-capability. A successfully demonstrated counter to enhanced command and control afforded by high-frequency radio communications was the employment of improved radio direction finding capability. Furthermore, experience shows that the most effective counter to RDF was strict adherence to radio silence. When this was ignored, the ramifications often proved decisive.

In May 1941, the German battleship *Bismarck* posed a significant threat to British shipping in the Atlantic Ocean. After an initial confrontation with the British fleet, resulting in the loss of *HMS Hood*, the German battleship, slightly damaged in the confrontation, sought to break contact with pursuing British naval units. The British considered “*Bismarck*’s destruction an imperative.”¹¹ On May 26, 1941, the captain of the *Bismarck*, confident that he had eluded the British warships, transmitted a lengthy message to Berlin to report his situation. The signal was detected by British RDF assets and the *Bismarck*’s position generally fixed. The Royal Navy converged upon the *Bismarck* and sank her.¹²

The Battle of the Atlantic did not end with the sinking of the *Bismarck*. With the entrance of the United States into the war, the sea lines of communication between the United States and Great Britain assumed strategic importance. The “wolf pack” technique employed by German submarines revealed one of the true dilemmas of emphasizing radio communications—how to weigh the value of the information obtained from transmitting against the risk to the originator of the transmission. This issue played itself out during the buildup of forces to invade the European continent.

Before that vast offensive could be mounted, the Allies had to win the Battle of the Atlantic. In this communications intelligence played a role of high importance. Indeed, in some respects the Battle of the Atlantic might be viewed as a duel between the Axis and the Allied cryptanalytic organizations. And while Donitz' B-Dienst had its successes, the Allied communications-intelligence agencies enjoyed the advantage of access to the extremely heavy traffic of the U-boat fleet.

In part, this stemmed from Donitz' insistence on maintaining tactical control of his submarines so as to concentrate them in wolf packs on the richest prizes. He was aware of the danger in all the talk, but, he contended, 'The signals from the U-boats contained the information upon which was based the planning and control of those combined attacks which alone held the promise of really great success against the concentrated shipping of any enemy convoy.' His encouragement of communication led to an almost complete relaxation of radio discipline. U-boats went on the air to report a toothache on board or to congratulate a friend at headquarters on a birthday. U-boat command became 'the most gabby military organization in all the history of war.'

Thanks to Commander Laurance F. Safford, head of OP-20-G and father of the Navy's communications-intelligence organization, the United States had, upon its entrance into the war, an Atlantic arc of high-frequency direction-finders to exploit the U-boat garrulity.¹³

The effective counter to German U-boat strategy was to first detect a U-boat's transmissions, obtain a fix, and then to attack and sink it. The allies utilized RDF to help ensure that for the U-boats, "There was no way of avoiding a fix except by maintaining radio silence."¹⁴ The Germans chose enhanced, centralized command and control over decentralized decisionmaking. This choice permitted allied RDF efforts to be decisive in the Battle of the Atlantic. It is worth noting the apparent and striking similarity between Grand Admiral Donitz' cited contention regarding enhanced command and control of the German U-boat fleet and the present capabilities offered by the networked, always-on force.

The period of the Cold War was marked by extraordinary advances in communications related capabilities and counter capabilities. Techniques of electronic warfare were continuously refined in order to obtain and maintain effective use of a contended electromagnetic spectrum. Pertinent to this paper is the recognition that during this period passive monitoring and analysis of radio transmissions continued to provide valuable information. Passive monitoring of the radio frequency spectrum yielded for the United States (and likely the Soviets, too) "a wealth of useful intelligence," including the seemingly obscure yet prized information derived from merely detecting telemetry data transmitted by Soviet ballistic missiles during firing tests.¹⁵

The Falklands campaign of 1982 potentially marked the beginning of the current desensitized attitude toward radio transmission security. Rear Admiral Woodward, Commander of the British Task Force, made a conscious decision not to maintain radio silence in order to compensate for the absence of Airborne Early Warning capability. He judged that the always-on radar and radio communications which afforded him local situational awareness offset the recognized risks incumbent with forgoing radio silence.

“I therefore assessed the balance of advantage lay with comprehensive communications between the British ships and aircraft, despite the risk of the Argentinians charting our whereabouts from them.”¹⁶

The same sentiment was not shared by Argentinian pilots, who on May 4, 1982, flew their Exocet missile equipped Etendards, “never daring to open up on their own radios,”¹⁷ attacked the British fleet, and succeeded in sinking HMS Sheffield.¹⁸

If the Falklands War, in modern times, introduced the notion that always-on, continuously emitting systems provide more security than what can be gained from maintaining radio silence, that presumption was not widely held until more than a decade later. It appears that an attitudinal change occurred coincident with the rapid increase in microprocessor technology overall, and the surge in widespread public adoption of the Internet, cellular phones, and personal digital assistants.

The US consumer and business communications environment of the 1990’s introduced a sense of urgency to get digitally connected. Widespread and rapidly growing use of Email, personal computing, and digital cellular telephony established new expectations for how information could and should be exchanged in a battlefield environment. Still, during the 1990’s, transmission security was stressed both in doctrinal field publications and training courses. For example, FM 24-33, dated 17 July 1990, states:

We must not operate our radios unnecessarily. Minimizing transmissions will safeguard our radios for critical transmissions.... We must never forget that operating our radios unnecessarily increases the enemy’s opportunities to gather information.¹⁹

And again, citing from a 1998 radio frequency communications training manual:

When a message is transmitted by radio, the originator may know some of those who are receiving it, but will never know all of those who are receiving the message. You must assume that an enemy receives every transmission. Properly prepared messages using modern cryptographic systems may prevent an enemy from understanding a message. However, they can still learn a lot. For example, as time for a planned operation approaches, the number of messages transmitted increases. An enemy then knows that something will occur soon, and their forces are alerted. Strict radio silence is the main defense against radio intelligence.²⁰

In the 1990's, doctrine continued to recognize and propound the lessons learned from the experience of previous years' wars. That experience was that enemy forces could and likely would seek actionable intelligence simply by means of passively detecting, analyzing, and processing radio transmissions received on the battlefield. In spite of this doctrinal recognition, three factors during this period appear to have substantially derailed the traditional respect for transmission security. The first was Operation Desert Storm which heralded the supremacy of U.S. technology on the battlefield. The second was rising expectations, driven by the consumer electronics industry, promising that anyone, anywhere, and at anytime could be connected with the information they wanted. And the third contributing factor was the introduction of transmission techniques which, at the time, were difficult to detect with legacy RDF and spectral analysis equipment. These three factors, in concert with the previous Falklands experience, laid the foundations for creating the networked, always-on force. The next war would validate many, if not all of the benefits envisioned for that force.

Operation Iraqi Freedom, which commenced in 2003, provided an opportunity to examine the Network Centric Warfare concept and its hypothesis that a "robustly networked force improves information sharing, collaboration, quality of information, and shared situational awareness resulting in significantly increased mission effectiveness."²¹ Case studies published by the Center for Strategic Leadership discuss in rich detail the remarkable battlefield capabilities achieved through the networking of forces. These capabilities have been validated in recent combat operations in Iraq. The robustly networked force yields exceptional flexibility and combat power, even if "always-on." The studies suggest that even more combat efficiency remains to be gained by further inter-connecting forces on the battlefield. On the other hand, these case studies do not overlook the fact that enemies of the future will adapt or have access to dual-use technologies. The recent experience in Iraq suggests that future enemies must, and therefore will, seek novel, asymmetrical approaches to reduce the combat effectiveness of the networked force in a dynamic information environment.

To conclude this section on historical experience it is instructive to glance at the very recent past. In the summer of 2006, Israeli military forces conducted operations in south Lebanon. In September 2006, after hostilities had ceased, reports emerged suggesting that "Hezbollah guerrillas were able to hack into Israeli radio communications."²² The reports proved inaccurate, or at least misleading. Hezbollah had not, apparently, intercepted and read Israeli tactical radio communications. James Bowden, the U.S. Army's senior program official for the Single-Channel Ground and Airborne Radio System (SINCGARS), clarified in an interview what actually took place:

“It’s not the hopping but the encryption that’s very difficult, if not impossible, to break. What they did is use direction finding [DF] to locate frequency hoppers. In fact, they’re easier to DF than conventional signals because you have more shots at it. With a commercially available system, you can probably find at least one of the frequencies.”²³

The Israeli military has not publicly commented on the impact of Hezbollah’s apparent success with RDF in these recent military operations. However, a former Israeli general, speaking on condition of anonymity, said “Hezbollah’s ability to secretly hack into military transmissions had ‘disastrous’ consequences for the Israeli offensive.”²⁴ Additionally, Nizar Qader, a retired Lebanese army general, has further stated that, “The information collected by signals intercepts was being used to help direct fighters on the battlefield.... These are tactics of a modern army.”²⁵

The experience from these recent findings show that passive RDF technologies combined with spectral analysis techniques continue to mature and adapt in tandem with modern radio transmission technologies. More revealing, perhaps, is the assertion that Hezbollah radio intelligence activities are the “tactics of a modern army.” This assertion, coming as it does from an insurgent-like military organization, illuminates the present global technological environment wherein the foundations of digital command and control systems are fabricated with dual-use technologies, those that have both commercial and military applications. The digital features of the modern battlefield have become almost indistinguishable from those of consumer electronics.

Leading to the Present Situation

Mentioned above were three factors that contributed during the 1990’s to a desensitized approach to transmission security. The present situation is explained by the evident convergence of military and consumer communications technology and a commitment to a style of warfare that emulates individual peacetime capability of being continually connected to digitized information.

The principle change in the communications environment over the past ten years has been the widespread adoption of digital technologies both in consumer electronics and in military command and control systems. In fact, many of these technologies are now shared, or dual-use, created by an Information Technology (IT) industry that caters to both global commercial and military markets. The CEO of Rambus, Inc., a company that provides microprocessor interface solutions for consumer computing and communications applications, recently stated, “The military used to drive electronics. Then, in the 1990’s, it changed. Today,

consumer electronics drives everything.”²⁶ A benefit of incorporating consumer electronics technology into military systems is cost savings. In an article addressing this relationship between military and consumer electronics, Geoffrey James found, “As they become more cost-conscious, defense electronics contractors are...drawing more heavily on existing commercial products to build the computing and communications infrastructure that will make NCW-enabled devices work together.”²⁷ And time to market is another advantage. Technology acquisition and fielding is quicker if it is both familiar and on the shelf.

It is difficult to overstate the impact of this convergence of consumer and military economies as it pertains to the digitized battlefield. Not only are many of the underlying digital technologies shared, but the intellectual acumen and propensity for innovation has been globalized.²⁸ In the last century one could expect to find technical expertise applicable to military purposes in relatively niche locations. These were principally to be found in government agencies, select universities, and also within corporations focused on technology research and development for government use. This is no longer the situation. The commonality of computing hardware and software between military command and control systems and commercial IT ensure that skilled knowledgeable workers with innovative insight useful in military applications can be found wherever commercial IT development takes place – virtually everywhere. This produces both benefits and risks. On the one hand, military technical requirements can be met faster while incorporating complex solutions at reduced cost. Evolution of the network-centric force illustrates how fast this process is taking place. On the other hand, potential enemies have access to the same technology development life-cycle from which they, too, can produce or refine a system to enhance their warfighting effectiveness.

Nations tend to make war the way they make wealth.²⁹ With this thought in mind, Colin Gray offers that:

The current policy on transformation, which at the DOD level at least, is very much a high technology story, is a direct reflection on the trends in American society....When America was predominately an industrial society, it waged industrial-age war on a scale in World War II that confounded foes and astonished allies. Now that America is evolving into a post-industrial society, wherein the manipulation of information is the key to prosperity, so, naturally enough, the Armed Forces must reflect that emerging reality.³⁰

A significant change over the past decade is found in the way America generates its wealth. A large cadre of corporate enterprise and technically savvy consultants has significant financial incentive to maintain a steady focus on technical solutions for meeting the challenges of modern warfare. In spite of its proven benefits, a potentially disruptive problem arises when, fixated on technology, US forces become overly dependent on a particular style of warfare. A

style of warfare characterized by a singular, pervasive, networked, and always-on force may be an example of this. In war, advantage can be gained from attacking a superior opponent's style of warfare. Given the historical record and the methods employed by adversaries in the Global War on Terrorism (GWOT), the American style of warfare is what enemies will seek to attack. Similar to technical methods employed by the Allies to defeat chatty German U-boats in World War II, passive RDF and spectral analysis provides asymmetrical fighters a technical avenue of approach toward defeating the American style of warfare.³¹

Vulnerabilities

The vulnerabilities evident from this discussion fall into three categories. First, a tactical vulnerability exists when enemies gain and use RDF technology for decisive effect. Second, at the operational level, a successful employment of passive RDF technology against U.S. forces exposes a vulnerability in the style of warfare U.S. forces are becoming dependent upon. And thirdly, from a strategic perspective, the disruptive employment of RDF and spectral analysis tools by potential adversaries illuminate the U.S. vulnerability of forfeiting to international competitors essential leadership in the development of key dual-use technologies.

Tactical Vulnerability

An emergent, if not already existent vulnerability for the networked, always-on force is that opposing forces will leverage the employment of available and obtainable technology to conduct passive and moderately sophisticated RDF and spectral analysis. Employed by asymmetrical fighters, these passive measures will increase their combat effectiveness and enhance their ability to achieve decisive results while operating in complex battle environments. Spectral analysis and RDF equipment is available from manufacturers around the globe. The equipment capabilities characteristically keep pace with advances in transmission techniques.

Broadband radio direction-finding receiver advances instantaneously enable coverage of a large bandwidth at high speed to locate radio frequency emissions. Direction finding is a key function in electronic warfare radio reconnaissance systems. Broadband direction finders are now capable of overcoming frequency-hopping, low-probability-of-intercept and low-probability-of-detection techniques.³²

Historical experience shows us that valuable information can be gained through passive monitoring of the radio spectrum. The Al Qaeda Training Manual recognizes the importance of information, stating that, "Information about the enemy's intention provides early warning signs for the command, which in turn makes appropriate preparation and thwarts the enemy's

opportunity.” And also, that “Information benefits the Organization’s command by providing information about movements of the enemy and his members.”³³

Asymmetric fighters characteristically favor passive means of gathering information. U.S. forces employ highly effective ISR assets which narrow the asymmetric fighter’s options for how he can securely gather intelligence. Radio spectral analysis and RDF techniques offer a means to act passively in order to detect always-on ISR systems and combat formations while locating soft or special targets.

The position can be maintained that adherence to “radio silence” is not necessary when troops are in contact with the enemy. When forces are engaged in combat any effort to maximize speed in the decisionmaking cycle trumps concealing friendly presence from the enemy. After all, the presence of friendly forces is revealed to the enemy when they are shooting at him. In traditional warfare, especially land warfare, this is a valid argument. However, a desensitized view toward, or worse, a blanket dismissal of the historical experience may be short-sighted. The preferred style of warfare chosen by enemies of the United States in the Global War on Terrorism (GWOT) is more similar to U-boat operations in the North Atlantic than maneuvering mechanized formations in open terrain. According the U.S. Marine Corps Combat Development Command’s document entitled, “Marine Corps Operations in Complex and Distributed Environments,”³⁴ likely adversaries:

- Will distribute their operations to exploit our vulnerabilities and indirectly erode our influence.
- Will try to mitigate our advantages by fighting in complex terrain (urban, mountain, jungle).
- Will seek to complicate operations by engaging in war among civilian populations.

These techniques are illustrative of an adversary who does not think like the commander of a mechanized rifle regiment. This adversary will choose to fight or flee based on detecting the presence of, and if possible, the composition of the force maneuvering against him. The sum of historical experience strongly suggests that against a networked, always-on adversary, RDF technology promises a path toward decisive results on the battlefield. Given its passive nature, employment of RDF lends itself to being supportive of urban fighting, terrorist actions, and asymmetric attacks.

Operational Vulnerability

In war, dependence on any a particular style of warfare is itself a vulnerability. The current trend is toward operational and tactical dependence on the network-centric, always-on style of

warfare. This dependence, combined with the aforementioned pervasive and desensitized attitude toward transmission security, has largely removed requirements to train in the absence of these systems.

And it is not only the guerrilla – the asymmetrical fighter, who does what is necessary, even illegal, to find a means to counter a competitive style of warfare. Developed nation states find opportunity, too. Quoting from the Office of the Secretary of Defense Report to Congress on the Military Power of the Peoples Republic of China (2006):

China continues to employ covert and illegal means to acquire foreign military and dual-use technology. Individuals allegedly engaged in illicit technology transfers to China were arrested in the United States and Russia in the fall of 2005.

China also continues to acquire key technologies and manufacturing methods independent of formal contracts. Industrial espionage in foreign research and production facilities and illegal transfers of technology are used to gain desired capabilities. Where technology targets remain difficult to acquire, foreign investors are attracted to China via contracts that are often written to ensure Chinese oversight, with the eventual goal of displacing foreigners from the companies brought into China.³⁵

The primary concern in the current environment is the methods cited for obtaining key technologies. These methods can readily be employed by rogue states and wealthy non-state actors seeking globally diffused technology or expertise. A style of warfare that is dependent on ubiquitous, always-on radio communications is vulnerable to being thwarted by an opposing style of warfare; a style enhanced through possession of instruments that passively detect and analyze all manner of radio frequency emissions.³⁶

Strategic Vulnerability

The fact that advanced technology is being developed and obtained, legally or illegally, through access to the global digital technology knowledge-base illuminates a larger, strategic vulnerability. The networked, always-on force maintains traditional battlefield supremacy in partnership with the broader US economy and in particular with the information technology industry. The IT industry is a cornerstone of the US economy and displays American ingenuity and technical acumen. A looming strategic predicament is a disadvantageous position from which to compete in the globalized IT marketplace with innovative ideas. Testifying in March 2007, before the U.S. Congress, Microsoft Chairman Bill Gates stated, “The U.S. cannot maintain its economic leadership unless our work force consists of people who have the knowledge and skills needed to drive innovation.... We simply cannot sustain an economy based on innovation unless our citizens are educated in math, science and engineering.”³⁷ Mr.

Gates' comments regarding education and competitive innovation appertain to US military capability. Military power made effective through dependence on technical enablers assumes preeminence in the application of math, science, and engineering. For several decades the US information technology industry, to include universities and research centers, have ensured the US capacity to wage war competitively; to dominate battlefields with networked information systems. However, absent an IT industry that continues to indisputably lead in innovation, reliance on technology for the effective employment of military power will prove detrimental.

A thorough discussion of the US economy's influence on strategic military capabilities is beyond the scope of this paper. Suffice to say that a leading-edge indicator of the strategic challenge will be the use of advanced, dual-use technology, sourced from outside the US, effectively employed in exploiting the always-on vulnerability of the networked force.

Potential Exploit

A foreseeable exploit is envisioned by a non-traditional fighting organization, perhaps insurgents, who are in possession of modern RDF and spectral analysis hardware, software, and processing capacity. This fighting organization is faced with -- maybe even surrounded by, a belligerent force constantly emitting radio frequency energy from every level of its organization. In this situation, two men take up temporary residence in a high-rise building near a coalition transportation hub. Over a period of time they observe and record patterns of signals (traffic analysis) and correlate these patterns with events later made public in the open media. They deduce from their observations and analysis that certain signals are present, others more pronounced, and still others disappear completely when high level U.S. political figures are passing through the transportation hub. With this intelligence, the two men are able to produce future unambiguous indicators based on real-time signal comparison in order to carry out an attack on a prominent U.S. political leader.

The example highlights what has been known since the dawn of radio: actionable intelligence can be collected and used by passively monitoring an enemy's transmissions. This intelligence can prove decisive. On a traditional battlefield, where formations maneuver against formations, detection of transmitted signals is of fleeting and often minor significance. However, for the fighter whose style of warfare necessitates he detect, avoid contact, and attack selectively; the ability to passively detect and analyze his opponent's use of the radio spectrum is of utmost significance. The asymmetrical fighter will employ passive RDF and spectral analysis against an always transmitting networked force because the opportunity exists. He

exploits the opportunity in order to more effectively plan his maneuver and executes to achieve decisive effect.

Recommendations

Three recommendations are advanced which entail understanding a potential adversary's opportunity given readily available technology, educating toward decentralized command and control, and development of a situational awareness architecture that is not dependent on maneuver force transmissions.

(1) Quantitative Investigation. First, a quantitative investigation must be made to demonstrate what a potential enemy can learn about U.S. forces with the same RDF and spectral analysis tools available in the global, commercial marketplace. There should be two primary objectives for this study. The first is to determine the limits of vulnerability and predict the most probable vulnerabilities an adversary will seek to exploit in order to enhance his style of warfare. These questions should be asked: "What information can be gathered using low-cost tools?" And, "What information can be gathered using moderately expensive commercial tools?" The second objective of this quantitative investigation should be to monitor the state of technological advancement in the marketplace with respect to RDF and spectral analysis technology. An accurate gauge of the level of pertinent technical diffusion throughout the marketplace is essential in order to shape training and forestall unnecessary fiscal waste.

(2) Train and Educate for Passive (Listen-only) Network Connectivity. Training should not neglect the historical experience. Radio silence, i.e. transmission security, may be required to close with and destroy an illusive, technically savvy foe. Individual and unit training, in concert with doctrinal methods, should include training which emphasizes decentralized action under the guidance of a commander's intent in the absence of transmitting detectable signals. Greater responsibility will need to be assumed at lower levels of command and leadership. Decisionmaking should be decentralized. The implications are for a level of training – and education, that enables units and individuals to operate in a predominately passively mode with respect to the larger, networked force. These units and individuals will still be in receipt of near-real-time battlefield situational awareness information via passive receipt of the data. However, their own systems will not auto-transmit, nor will transmissions be initiated until a tactical decision cycle necessitates.

(3) A Technical Solution. Technology may evolve to eliminate detectable communicative transmissions on the battlefield. Research should continue which leads to the fielding of truly covert, undetectable wave-forms for non-line-of-sight communications. But this research should

not be the main effort. The global information technology environment will produce an antidote in short order given the convergence of defense and commercial related research and development in wireless technologies.

The preferred technical approach is to develop and field a primarily passive, digitized battlefield situational awareness architecture. This approach reaffirms the importance of transmission security on the battlefield, does not have to be more expensive, and can be equally effective for command and control of the networked force. The essence of this proposed architecture is that it leverages stand-off ISR capability to identify--and gather other information, about friendly forces rather than being dependent on transmissions from the units or individuals themselves. The collected data is combined and correlated and broadcast to the larger force, which in turn receives the information passively. Of course, the enemy force situation is combined and broadcast along with the ISR collected friendly force situation. The networked force need not remain "always-on" and certainly not all of it all the time. Since much of the force will be trained, educated, and conditioned to operate in receive-only mode, vulnerabilities susceptible to exploitation by RDF and spectral analysis techniques can be minimized. With this architecture, command and control effectiveness is not reduced when maneuver units choose to maintain "radio silence." When a situation requires transmission (which might be frequently, but not "always-on") the unit or individual transmits. This primarily passive battlefield situational awareness architecture is an enabler for a professionally educated force; decentralized and controlled first through the commander's intent.

Conclusion

Historical experience, together with recent experience, serves to refresh the reality that technology is only an enabler and does not guarantee winning at war. Furthermore, when a style of warfare becomes dependent on a type of technology, as the German U-boat style of warfare became dependent on frequent radio transmissions to satisfy command and control requirements, a technical antidote is devised increasing the risk for defeat. Colin Gray warns that "The principle danger in the years immediately ahead is that U.S. Armed Forces will be so committed to their own network-centric transformation, that they fail to recognize the true character of potentially effective offsetting revolutionary change elsewhere."³⁸ The use of passive spectral analysis and RDF techniques by asymmetrical fighters will not represent, in and of itself, a revolutionary change, certain to offset the capabilities of the networked force. However, these techniques, adroitly employed to assist in achieving decisive effect, are indicative of a contemporary military enlightenment³⁹ well underway among our potential and

actual adversaries. The revolutionary change is that their enlightenment finds its strength to flourish in the same global marketplace of ideas, digital technology, and innovation which has enabled ours.

Advanced military digital command and control systems are inseparably converged with the global information technology industry. Radio direction finding and spectral analysis techniques in the hands of the asymmetric fighter will present new challenges for the American style of warfare. The capacity for innovative, creative leadership combined with genuine professional development must be strengthened and expanded. For US military forces, this requires a regimen of training and education that ensures military success in the absence of always-on communications.

Endnotes

¹ Mohamad Bazzi, "Hezbollah cracked the code; Technology likely supplied by Iran allowed guerrilla to stop Israeli tank assaults," *New York Newsday*, 19 September 2006 [database on-line]; available from Lexis-Nexis; accessed 27 December 2006.

² John B. Tisserand III, *Network Centric Warfare Case Study: U.S. V Corps and 3rd Infantry Division (Mechanized) during Operation Iraqi Freedom Combat Operations (March to April 2003) Volume III: Network Centric Warfare Insights* (Carlisle Barracks, PA: U.S. Army War College, 28 August 2006), 21.

³ U.S. Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication JP 1-02 (Washington, D.C.: U.S. Department of Defense, 12 April 2001, Amended through 8 August 2006), 548.

⁴ Tisserand, C-1.

⁵ Donald H. Rumsfeld, *The National Defense Strategy of the United States of America* (Washington, D.C.: U.S. Department of Defense, 2005), 5.

⁶ U.S. Joint Chiefs of Staff, Richard B. Myers, Chairman, *National Military Strategy of the United States of America* (Washington, D.C.: U.S. Department of Defense, 2004), 6.

⁷ Colin S. Gray, *Recognizing and Understanding Revolutionary Change in Warfare: The Sovereignty of Context* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2006), 46.

⁸ Abraham Marcus and William Marcus, Ralph Horton, ed., *Elements of Radio* (New York: Prentice-Hall, 1948), 5.

⁹ Joseph D. Modell, *Transmitter Hunting: Radio Direction Finding Simplified* (New York: McGraw-Hill, 1987), 1-3.

¹⁰ Anthony Brown, *Bodyguard of Lies: The Extraordinary True Story Behind D-Day* (Guilford, CT: The Lions Press, 2002), 22.

¹¹ Ibid., 56.

¹² Ibid.

¹³ David Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet* (New York: Scribner, 1996), 504-5.

¹⁴ Ibid., 270.

¹⁵ Dr. Alfred Price, *War in the Fourth Dimension* (London: Greenhill Books and Mechanicsburg, PA: Stackpole Books, 2001), 25.

¹⁶ Admiral Sandy Woodward with Patrick Robinson, *One Hundred Days: The Memoirs of the Falklands Battle Group Commander* (Annapolis, MD: Naval Institute Press, 1997), 3.

¹⁷ Ibid., 5.

¹⁸ Ibid., 3-20.

¹⁹ U.S. Department of the Army, *Communications Techniques: Electronic Counter-Countermeasures*, Army Field Manual FM 24-33 (Washington, D.C.: U.S. Department of the Army, 17 July 1990), Ch. 2, Sec. 2-1 b.

²⁰ U.S. Department of the Navy, *Navy Electricity and Electronics Training Series Module 17—Radio-Frequency Communications Principles*, Navy Publication NAVEDTRA 14189, September, 1998) 3-37.

²¹ Tisserand, 1.

²² Bazzi.

²³ David A. Fulghum, "Doubt As a Weapon; Lebanon fighting produced an information warfare coup for Hezbollah and Iran," *Aviation Week & Space Technology*, 27 November 2006 [database on-line]; available from Lexis-Nexis; accessed 27 December 2006.

²⁴ Bazzi.

²⁵ Ibid.

²⁶ "We Finally Get our Paws on PlayStation 3," *IEEE Spectrum Online*, 20 December 2006 [journal on-line]; available from <http://spectrum.ieee.org/dec06/comments/1668>; Internet; accessed 29 March 2007.

²⁷ Geoffrey James, "The war at home; How the war in Iraq is changing the relationship between defense and commercial electronics," *Electronic Business*, 1 January 2006 [database on-line]; available from Lexis-Nexis; accessed 27 December 2006.

²⁸ The International Monetary Fund's proposed definition for globalization is "the growing economic interdependence of countries world-wide through the increasing volume and variety of cross-border transactions in goods and services and of international capital flows, and also through the more rapid and widespread diffusion of technology." See Terrence R. Guay, *Globalization and Its Implications for the Defense Industrial Base* (Carlisle Barracks, PA: U.S. Army War College, February 2007), 1.

²⁹ Alvin Toffler and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston: Little, Brown, 1993), 3.

³⁰ Gray, 20.

³¹ Ibid., 43.

³² Clarence A. Robinson Jr., "Position Fixing Methods Use Broadband Direction Finders," *Signal*, October, 1998 [database-online]; available from ProQuest; accessed 27 December 2006.

³³ Jerrold M. Post, M.D., ed., *Military Studies in the Jihad against the Tyrants: The Al-Qaeda Training Manual* (Maxwell AFB, AL: USAF Counterproliferation Center, 2004), 86.

³⁴ Lt. Gen. James F. Amos, "Marine Corps Operations in Complex and Distributed Environments," 11 January 2007; available from http://www.mcw.quantico.usmc.mil/file_download.cfm?filesource=c:%5CMCWL_Files%5CC_P%5CDistributed%20Operations%20Summary%20dtd%20011107.pdf; Internet; accessed 29 March 2007.

³⁵ Office of the Secretary of Defense, *Annual Report to Congress – Military Power of the People's Republic of China 2006* (Washington, D.C.: U.S. Department of Defense), 6, 22.

³⁶ Geoffrey James captures how advanced technology becomes available when he states, "...the need to make NCW happen quickly, at a reasonable cost, increases the speed with which technology gets transferred to the commercial sector. This, in turn, means that mainstream semiconductor firms will be able to bring commercial products based on NCW-related technology to the market far sooner than would otherwise be possible."

³⁷ Associated Press, "Gates Voices Concern About U.S. Education," *New York Times*, 8 March 2007 [newspaper on-line]; available from <http://www.nytimes.com/2007/03/08/business/08gates.html?ei=5088&en=db607b26877228ae&ex=1331010000&partner=rssnyt&emc=rss&pagewanted=all>; Internet; accessed 29 March 2007.

³⁸ Gray, 14.

³⁹ Colin Gray states, "It is difficult for a proud and self-confidently dominant military power to accept the notion that there can be more than one contemporary military enlightenment", Gray, 24.